

(ii) Any time after the expiration of the opt-out period but before solicitations that would have been prohibited by the expired opt-out are made to the consumer.

(2) *Combination with annual privacy notice.* If you provide an annual privacy notice under the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., providing a renewal notice with the last annual privacy notice provided to the consumer before expiration of the opt-out period is a reasonable period of time before expiration of the opt-out in all cases.

(d) *No effect on opt-out period.* An opt-out period may not be shortened by sending a renewal notice to the consumer before expiration of the opt-out period, even if the consumer does not renew the opt out.

**§ 680.28 Effective date, compliance date, and prospective application.**

(a) *Effective date.* This part is effective January 1, 2008.

(b) *Mandatory compliance date.* Compliance with this part is required not later than October 1, 2008.

(c) *Prospective application.* The provisions of this part shall not prohibit you from using eligibility information that you receive from an affiliate to make solicitations to a consumer if you receive such information prior to October 1, 2008. For purposes of this section, you are deemed to receive eligibility information when such information is placed into a common database and is accessible by you.

**PART 681—IDENTITY THEFT RULES**

Sec.

681.1 Duties regarding the detection, prevention, and mitigation of identity theft.

681.2 Duties of card issuers regarding changes of address.

APPENDIX A TO PART 681—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

AUTHORITY: Public Law 108–159, sec. 114; 15 U.S.C. 1681m(e).

SOURCE: 72 FR 63771, Nov. 9, 2007, unless otherwise noted.

**§ 681.1 Duties regarding the detection, prevention, and mitigation of identity theft.**

(a) *Scope.* This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

(b) *Definitions.* For purposes of this section, and Appendix A, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage

## Federal Trade Commission

## § 681.2

brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program*—(1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in appendix A of this part and include in its Program those guidelines that are appropriate.

[74 FR 22645, May 14, 2009]

### § 681.2 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 681.1(a) that issues a debit or credit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of